

Relay Placement for Physical Layer Security: A Secure Connection Perspective

Jianhua Mo, Meixia Tao, *Senior Member, IEEE*, and Yuan Liu, *Student Member, IEEE*

Abstract—This work studies the problem of secure connection in cooperative wireless communication with two relay strategies, decode-and-forward (DF) and randomize-and-forward (RF). The four-node scenario and cellular scenario are considered. For the typical four-node (source, destination, relay, and eavesdropper) scenario, we derive the optimal power allocation for the DF strategy and find that the RF strategy is always better than the DF to enhance secure connection. In cellular networks, we show that without relay, it is difficult to establish secure connections from the base station to the cell edge users. The effect of relay placement for the cell edge users is demonstrated by simulation. For both scenarios, we find that the benefit of relay transmission increases when path loss becomes severer.

Index Terms—Relay placement, physical layer security, secure connection, outage.

I. INTRODUCTION

Wireless communication is inherently vulnerable to eavesdropping due to its broadcast nature. However, by exploiting the randomness of the wireless propagation channels, we can enhance the security in physical layer [1]. On the other hand, cooperative relay has received much attentions due to its ability of power reduction, coverage extension, and throughput enhancement. Thus, it is attractive and promising to utilize these benefits for physical layer security.

The authors in [2] discussed the four-node (source, destination, relay, eavesdropper) secure communication system from an information-theoretical perspective and studied several relay strategies, such as decode-and-forward (DF) and noise-forwarding (NF). Authors in [3] investigated the secrecy rate maximization problem for the four-node system in multicarrier relay channel with the DF strategy. For the secure transmission system with multiple relays, the beamforming and relay selection was considered in [4] and [5] respectively under the assumption that the eavesdropper only wiretaps the second hop during the cooperative transmission. A joint problem of secure resource allocation and scheduling was studied in [6] for cellular networks with DF relays.

In [7], the authors proposed another relay strategy in which the relays add independent randomization in each hop (we refer it as randomize-and-forward (RF)). It was proved therein that under the RF strategy, securing each individual hop is

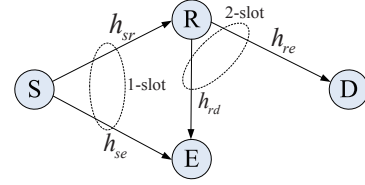


Fig. 1. An illustration of the four-node system model, where S , R , D , and E represent the source, relay, destination, and eavesdropper, respectively.

sufficient for securing the end-to-end transmission. Scaling law of secrecy capacity were then obtained by using such RF strategy in [7]. The authors in [8] analyzed the maximal number of eavesdroppers that can be tolerated in the two-hop secure transmission with jamming when RF strategy was used.

Our paper is motivated twofold. First, though the cooperative secure transmission has been studied in several scenarios (e.g., [2]–[9]), to our best knowledge, no attempt has been made to study relay placement for physical layer security. Second, although fading was utilized to achieve physical layer security (e.g., [10]), there is no theoretical analysis about the impacts of large scale path loss on security.

The main contributions of this work are summarized as follows. 1) In the four-node system, we derive the optimal power allocation for the DF strategy and find that the RF strategy is always better than the DF in terms of secure connection probability. 2) We show that when the eavesdropper is far away, placing the relay at the midpoint of the source and the destination is asymptotical optimal, and the outage probability of the RF strategy is about half of the DF. 3) In cellular networks, we derive the secure outage probability without relay and show the superiority of placing RF relay over DF relay through simulation. 4) We analyze the effects of path loss on secure connection and find that relay transmission achieves more benefit when path loss is severer.

II. MAIN RESULTS

We consider two scenarios, i.e., the four-node system and cellular networks. For both scenarios, we assume that the cooperative transmission consists of two phases. During the first phase, the source (or base station (BS)) transmits while the relay (or relay station (RS)) listens. During the second phase, the relay transmits and the destination (or mobile user (MU)) listens. The eavesdropper overhears in both phases. Here we assume that the direct link from the source (or BS) to the destination (or MU) is not available. The wireless fading channels are modeled by large-scale fading with path loss exponent α and small-scale block Rayleigh fading.

Notations: Subscripts s , r , d and e represent the source (or BS), relay (or RS), destination (or MU) and eavesdropper,

Manuscript received March 16, 2012; revised April 5, 2012. The associate editor coordinating the review of this letter and approving it for publication was Kai Kit Wong.

The authors are with the Dept. of Electronic Engineering, Shanghai Jiao Tong University, P. R. China(email:{mjh, mxtao, yuanliu}@sjtu.edu.cn).

This work is supported by the Innovation Program of Shanghai Municipal Education Commission under grant 11ZZ19 and the Joint Research Fund for Overseas Chinese, Hong Kong and Macao Young Scholars under grant 61028001.

$$P_{DF}(\mathbf{d}) = 1 - \frac{d_{se}^\alpha d_{re}^\alpha}{(d_{rd}^\alpha + d_{re}^\alpha)(d_{sr}^\alpha + d_{se}^\alpha) + d_{sr}^\alpha d_{rd}^\alpha + \frac{p_r d_{sr}^\alpha}{p_s}(d_{sr}^\alpha + d_{se}^\alpha) + \frac{p_s d_{rd}^\alpha}{p_r}(d_{rd}^\alpha + d_{re}^\alpha)}. \quad (6)$$

respectively. d_{ij} and h_{ij} denote the distance and channel coefficient between node i and j , respectively. p_s and p_r denote transmit powers of the source and relay, respectively. For brevity, we denote $\mathbf{d} := \{d_{sr}, d_{rd}, d_{se}, d_{re}\}$ and $\mathbf{p} := \{p_s, p_r\}$.

A. Four-node System

In this subsection, we study a four-node system consisting of a source, a destination, an eavesdropper and a relay shown in Fig. 1. Both DF and RF strategies are analyzed in terms of secure connection probability. Here the knowledge of channel state information (CSI) for the eavesdropper is assumed to be known as the eavesdropper may be another legitimate user who transmits signals but is not allowed to receive the confidential message from the source [10].

1) *Decode-and-Forward (DF)*: For the DF strategy, the relay uses the same codebook as the source's. The achievable rate from the source to the destination is given by

$$R_d = \frac{1}{2} \min \left\{ \log_2 \left(1 + \frac{p_s |h_{sr}|^2}{d_{sr}^\alpha} \right), \log_2 \left(1 + \frac{p_r |h_{rd}|^2}{d_{rd}^\alpha} \right) \right\}. \quad (1)$$

The eavesdropper wiretaps and combines the signals from both two hops, and as such the information rate at the eavesdropper is

$$R_e = \frac{1}{2} \log_2 \left(1 + \frac{p_s |h_{se}|^2}{d_{se}^\alpha} + \frac{p_r |h_{re}|^2}{d_{re}^\alpha} \right). \quad (2)$$

The secrecy rate of the system is

$$R_s = \max \{R_d - R_e, 0\}. \quad (3)$$

Similar to [11], [12], we define that the connection between the source and destination is secure if $R_s > 0$. Then the secrecy outage probability can be defined as

$$P_{DF}(\mathbf{d}, \mathbf{p}) = \Pr(R_s < 0) \\ = \Pr \left(\min \left\{ \frac{p_s |h_{sr}|^2}{d_{sr}^\alpha}, \frac{p_r |h_{rd}|^2}{d_{rd}^\alpha} \right\} < \frac{p_s |h_{se}|^2}{d_{se}^\alpha} + \frac{p_r |h_{re}|^2}{d_{re}^\alpha} \right).$$

Proposition 1. *For the DF strategy, the optimal power allocation satisfies*

$$\frac{p_r}{p_s} = \sqrt{\frac{d_{rd}^\alpha (d_{rd}^\alpha + d_{re}^\alpha)}{d_{sr}^\alpha (d_{sr}^\alpha + d_{se}^\alpha)}}, \quad (4)$$

and the minimal outage probability, denoted as $P_{DF}(\mathbf{d})$, is

$$P_{DF}(\mathbf{d}) = 1 - \frac{d_{se}^\alpha d_{re}^\alpha}{(\sqrt{(d_{sr}^\alpha + d_{se}^\alpha)(d_{rd}^\alpha + d_{re}^\alpha)} + \sqrt{d_{sr}^\alpha d_{rd}^\alpha})^2}. \quad (5)$$

Proof: Note that $\frac{p_s |h_{sr}|^2}{d_{sr}^\alpha}$, $\frac{p_r |h_{rd}|^2}{d_{rd}^\alpha}$, $\frac{p_s |h_{se}|^2}{d_{se}^\alpha}$ and $\frac{p_r |h_{re}|^2}{d_{re}^\alpha}$ are exponential distributed with means $\frac{p_s}{d_{sr}^\alpha}$, $\frac{p_r}{d_{rd}^\alpha}$, $\frac{p_s}{d_{se}^\alpha}$ and $\frac{p_r}{d_{re}^\alpha}$, respectively. Through some derivation, the outage probability is (6) on the top of this page. Using the inequality of arithmetic and geometric means, we get (4) and (5). ■

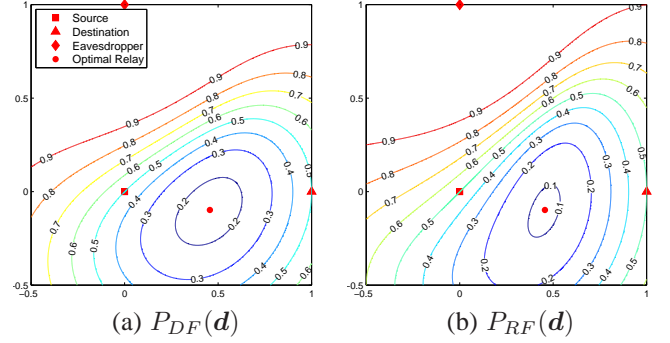


Fig. 2. The outage probability as a function of the position of DF and RF relay. The source, destination and eavesdropper are at (0, 0), (1, 0) and (0, 1), respectively and $\alpha = 4$. The optimal DF and RF relay positions are both around (0.4551, -0.0987) with minimal $P_{DF}(\mathbf{d}) \approx 0.1645$ and $P_{RF}(\mathbf{d}) \approx 0.0878$ while $P_{Direct}(\mathbf{d}) = 0.5$.

Proposition 1 shows that, to minimize the outage probability, only the power ratio $\frac{p_r}{p_s}$ matters rather than the absolute power.

2) *Randomize-and-Forward (RF)*: For the RF strategy, the source and relay use different codebooks to transmit the secret message. According to [7], the message is secured if the two hops are both secured. Thus the outage probability can be defined as

$$P_{RF}(\mathbf{d}) = 1 - \Pr \left(\frac{|h_{sr}|^2}{d_{sr}^\alpha} > \frac{|h_{se}|^2}{d_{se}^\alpha} \right) \Pr \left(\frac{|h_{rd}|^2}{d_{rd}^\alpha} > \frac{|h_{re}|^2}{d_{re}^\alpha} \right) \\ = 1 - \frac{d_{se}^\alpha d_{re}^\alpha}{(d_{sr}^\alpha + d_{se}^\alpha)(d_{rd}^\alpha + d_{re}^\alpha)}. \quad (7)$$

(7) shows that for the RF strategy, the source and relay powers do not influence the outage probability, which is different from DF.

Since neither (5) nor (7) is a convex function of the relay position, we resort to numerical results. In Fig. 2, we plot $P_{DF}(\mathbf{d})$ and $P_{RF}(\mathbf{d})$ as functions of the relay position. We find that the optimal positions of the DF and RF relays are both near to the midpoint of the source and destination. Moreover, the RF strategy is better than the DF strategy.

Theorem 1. *For the four-node system, the outage probability of the DF strategy is always larger than that of RF strategy.*

Proof: Observing (5) and (7), we have

$$\sqrt{\frac{1}{1 - P_{DF}(\mathbf{d})}} = \sqrt{\frac{1}{1 - P_{RF}(\mathbf{d})}} + \sqrt{\frac{d_{sr}^\alpha d_{rd}^\alpha}{d_{se}^\alpha d_{re}^\alpha}}. \quad (8)$$

Thus, $P_{DF}(\mathbf{d}) > P_{RF}(\mathbf{d})$ and Theorem 1 is proved. ■

Proposition 2. *When the eavesdropper is far away from the*

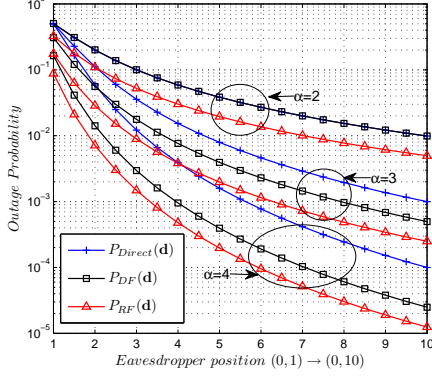


Fig. 3. Outage probability vs the eavesdropper's position. The source and destination are at (0, 0) and (1, 0), respectively. For every given eavesdropper's position, we find the optimal relay position and the corresponding minimal outage probability by numerical search.

source and destination,¹ the asymptotic optimal relay position is at the midpoint of the source and destination and

$$P_{RF}(d) \approx \frac{1}{2} P_{DF}(d) \approx \frac{1}{2^{\alpha-1}} P_{Direct}(d), \quad (9)$$

where $P_{Direct}(d) = \frac{d_{sd}^\alpha}{d_{sd}^\alpha + d_{se}^\alpha} \approx \frac{d_{sd}^\alpha}{d_{se}^\alpha}$ is the outage probability of direct transmission.

Proof: By (5) and (7), if $d_{se} \gg d_{sr}$ and $d_{re} \gg d_{rd}$,

$$P_{DF}(d) \approx \left(\sqrt{\frac{d_{sr}^\alpha}{d_{se}^\alpha}} + \sqrt{\frac{d_{rd}^\alpha}{d_{re}^\alpha}} \right)^2 \approx \left(\sqrt{\frac{d_{sr}^\alpha}{d_{se}^\alpha}} + \sqrt{\frac{d_{rd}^\alpha}{d_{se}^\alpha}} \right)^2 \quad (10)$$

$$P_{RF}(d) \approx \frac{d_{sr}^\alpha}{d_{se}^\alpha} + \frac{d_{rd}^\alpha}{d_{re}^\alpha} \approx \frac{d_{sr}^\alpha}{d_{se}^\alpha} + \frac{d_{rd}^\alpha}{d_{se}^\alpha}. \quad (11)$$

To minimize (10) and (11), we should have

$$d_{sr} = d_{rd} = \frac{1}{2} d_{sd}. \quad (12)$$

Thus, the Proposition 2 follows. ■

Fig. 3 shows the outage probabilities when the eavesdropper moves away from the source and destination. In this figure, the asymptotic results of Proposition 2 are verified. It is first observed that the outage probability of the RF strategy is indeed about half of the DF. In addition, as the path loss exponent α increases, more benefit can be achieved from relay transmission. Notice that $P_{DF}(d) \approx P_{Direct}(d)$ if $\alpha = 2$, meaning that DF relay transmission, compared with direct transmission, brings no benefit at this time!

B. Cellular Networks

We now consider a single-cell cellular network shown in Fig. 4. The hexagonal microcell is approximated as a circular cell of radius R with a BS at the center of the cell. The MUs aim to get a secure connection with the BS. Only downlink is considered and uplink transmission can be encrypted by the key transmitted through the secure downlink. The eavesdroppers, which may be other MUs, do not cooperate and are

¹This scenario is applicable when the eavesdropper can not come closer to the legitimate nodes than a specified distance or when each legitimate node is able to physically inspect its surroundings and deactivate the nearby eavesdroppers [11].

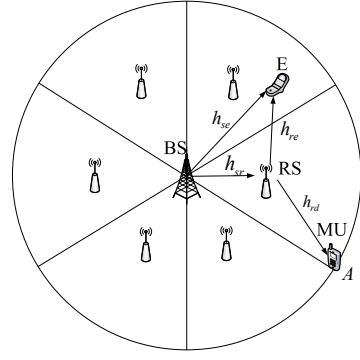


Fig. 4. An example of cellular networks with 6 sectors and RS's. The RS's are placed on the angle bisector of each sector.

uniformly distributed within the cell. Therefore, the knowledge of CSI for the eavesdroppers are not needed.

Proposition 3. If there exist N non-cooperative eavesdroppers uniformly distributed in the cellular networks, the outage probability for direct transmission, P_{Direct}^N , satisfies

$$P_{Direct}^1(d_{sd}) \leq P_{Direct}^N(d_{sd}) \leq 1 - (1 - P_{Direct}^1(d_{sd}))^N, \quad (13)$$

where $P_{Direct}^1(d_{sd})$ is the outage probability with single eavesdropper and given by

$$P_{Direct}^1(d_{sd}) = x^2 \sum_{k=0}^{\infty} \frac{(-1)^k}{1 + \frac{k\alpha}{2}} \left(\frac{1}{x^2} \right)^{1 + \frac{k\alpha}{2}} \quad (14)$$

$$= \begin{cases} x^2 \ln \left(1 + \frac{1}{x^2} \right) & \text{when } \alpha = 2 \\ 2x^2 \left(\frac{1}{6} \ln \frac{(x^2 - x + 1)}{(x + 1)^2} + \frac{1}{\sqrt{3}} \left(\arctan \frac{2 - x}{\sqrt{3}x} + \frac{\pi}{6} \right) \right) & \text{when } \alpha = 3 \\ x^2 \arctan \left(\frac{1}{x^2} \right) & \text{when } \alpha = 4 \end{cases}$$

with $x = d_{sd}/R$ is the normalized distance between the BS and MU.

Proof: The probability density function of d_{sd} is

$$f(d_{sd}) = \frac{2d_{sd}}{R^2}, \quad 0 \leq d_{sd} \leq R. \quad (15)$$

We then can prove (14) by integrating

$$P_{Direct}^1(d_{sd}) = \int_0^R \Pr \left(\frac{|h_{sd}|^2}{d_{sd}^\alpha} < \frac{|h_{se}|^2}{d_{se}^\alpha} \right) f(d_{se}) dd_{se}.$$

For (13), the left inequality is obvious. For the right one,

$$\begin{aligned} P_{Direct}^N(d_{sd}) &= \mathbb{E}_{\{d_{se_i}, 1 \leq i \leq N\}} \left\{ \Pr \left(\frac{|h_{sd}|^2}{d_{sd}^\alpha} < \max_i \frac{|h_{se_i}|^2}{d_{se_i}^\alpha} \right) \right\} \\ &= \mathbb{E}_{\{d_{se_i}, 1 \leq i \leq N\}} \left\{ 1 - \Pr \left(\bigcap_{i=1}^N \left(\frac{|h_{sd}|^2}{d_{sd}^\alpha} > \frac{|h_{se_i}|^2}{d_{se_i}^\alpha} \right) \right) \right\} \\ &\stackrel{(a)}{\leq} \mathbb{E}_{\{d_{se_i}, 1 \leq i \leq N\}} \left\{ 1 - \prod_{i=1}^N \Pr \left(\frac{|h_{sd}|^2}{d_{sd}^\alpha} > \frac{|h_{se_i}|^2}{d_{se_i}^\alpha} \right) \right\} \\ &= 1 - (1 - P_{Direct}^1(d_{sd}))^N, \end{aligned}$$

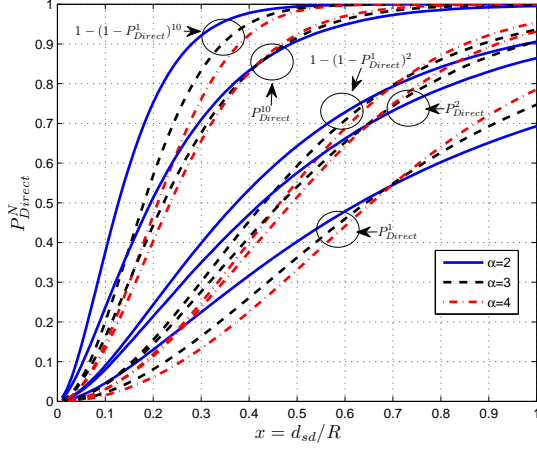


Fig. 5. Outage probability vs the normalized distance between the BS and MU.

where e_i denotes the i th eavesdropper and \mathbb{E} represents expectation. The inequality (a) is obtained by using conditional probability. This completes the proof of Proposition 3. ■

P_{Direct}^N can be obtained from numerical simulation. We plot P_{Direct}^N and $1 - (1 - P_{Direct}^1)^N$ in Fig. 5. First, we observe that P_{Direct}^N increases very fast with N , meaning that only a few non-cooperative eavesdroppers will block nearly all the secure connections from the BS to MU. Second, the outage probability is decreasing with α when x is small while increasing when $x \approx 1$. Interestingly, it suggests the MUs near the BS prefer severer path loss while the MUs near the cell edge prefer milder path loss. Finally, for the cell edge MUs, i.e., $d_{sd} = R$, we have

$$P_{Direct}^1(R) = \begin{cases} \ln 2 \approx 0.693 & \text{when } \alpha = 2 \\ \frac{2\pi}{3\sqrt{3}} - \frac{2}{3} \ln 2 \approx 0.747 & \text{when } \alpha = 3 \\ \frac{\pi}{4} \approx 0.785 & \text{when } \alpha = 4 \end{cases}$$

It shows that the cell edge MUs have no secure connections to the BS with very high probability.

To deal with this issue, we then propose a heuristic relay placement strategy as follows. The cell is first partitioned to M sectors and MUs in every sector is served by a relay as depicted in Fig. 4. Obviously, the MUs located at both the cell edge and sector edge, like point A (see Fig. 4), have the largest outage probability. As $P_{Direct}^N(R)$ has the upper bound $1 - (1 - P_{Direct}^1(R))^N$, we consider only one eavesdropper and aim to minimize $P_{Direct}^1(R)$. We then search the optimal relay position and power to minimize the outage probability of such MUs by numerical simulation.

We show the numerical results in Fig. 6 where $M = 6$, $N = 1$, and each relay has the power constraint $p_r \leq p_s$. It is shown that in such cases, RF is better than direct transmission while DF is inferior to direct transmission. Moreover, the outage probability of direct transmission of the MUs at point A is increasing with the path loss exponent α , while the outage probability with DF or RF relay decrease with α . Finally, the best relay position approaches to the cell edge as α increases.

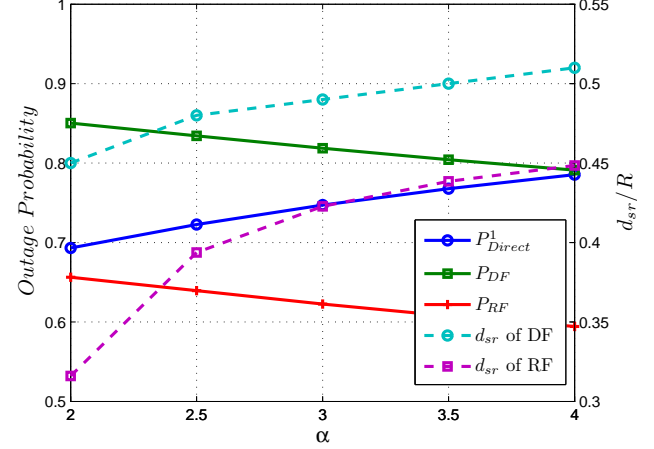


Fig. 6. Outage probability of MU located at point A and the position of relay vs path loss exponent with one eavesdropper.

III. CONCLUSION

In this paper, we have considered relay placement for secure connection problem. Through analytical expressions and numerical results, we have shown that relay is beneficial for establishing secure connection for the four-node system and cellular networks. We also found that relay transmission is especially helpful when path loss is severer. Furthermore, it was shown that the RF relay strategy, by introducing different randomization in each hop, is much better than the traditional DF relay strategy.

REFERENCES

- [1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.
- [2] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.
- [3] C. Jeong and I.-M. Kim, "Optimal power allocation for secure multi-carrier relay systems," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5428–5442, Nov. 2011.
- [4] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
- [5] I. Krikidis, J. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.
- [6] D. Ng, E. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3528–3540, Oct. 2011.
- [7] O. O. Koyluoglu, C. E. Koksul, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, 2012, to appear.
- [8] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 2067–2076, Dec. 2011.
- [9] P. Popovski and O. Simeone, "Wireless secrecy in cellular systems with infrastructure-aided cooperation," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 2, pp. 242–256, Jun. 2009.
- [10] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
- [11] P. Pinto, J. Barros, and M. Win, "Secure communication in stochastic wireless networks – Part I: Connectivity," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.
- [12] X. Zhou, R. Ganti, and J. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.